Security in Computing & IT
Revision Questions

LECTURE 1

- Explain the following four terms in one sentence each: confidentiality, privacy, integrity, availability and authenticity of information.
  - **Confidentiality:** The information can only be read/acquired by authorised users.
  - **Privacy:** Only authorised users can disclose legally obtained data to secondary users.
  - **Integrity:** Unauthorised users cannot alter/modify the information.
  - **Availability:** Authorised users can access/utilise the information.
  - **Authenticity:** The information comes from a verifiable source of origin.

- What is security by obscurity and what is security by legislation?

  Security by **obscurity** hides internal working and sensitive components essentially keeps the delicate details hidden. Security by **legislation** lets the laws prescribe allowable user activities, but the efficacy is limited as the offender may be in another jurisdiction, therefore better off as an additional method (e.g. violators are prosecuted or handed over to the police.

- What is a covert channel? Explain it on a simple example.

  Covert channel is data that has a subliminal meaning; the existence or absence of the data carries information, the actual value is irrelevant. For example, data hiding in the OSI model where it appears to be a packet carrying ordinary information, when in fact it is concealing its actual data in one of the several control fields in the TCP/IP headers.

- What is the difference between a security policy and a security mechanism?

  A **security policy** describes the aims of protection (e.g. only authorised users can access the resources), while a **security mechanism** implements the policy (e.g. users need to log in to qualify as authorised).

LECTURE 2

- What is a security mechanism? Give an example of it.

  A **security mechanism** is a means of implementing the security policies, for example implementing protected rooms, and access control.

- What are the security tradeoffs?

  Security trade-off is a balance achieved from two desirable but incompatible factors; a compromise between two risks.

- How can you measure risk?

  We can measure risk using the Common Vulnerability Scoring System (**CVSS**). It is based on a number metric in three main categories: Base (Immutable features of a core vulnerability), Temporal (Evolves during the lifetime of the vulnerability), and Environmental (How the vulnerability affects a particular installation).

- What is the difference between pervasive and specific security mechanisms? Give an example for each.

  Pervasive security mechanisms are not specific to any particular security service and are in general directly related to the level of security required, such as trusted functionality, security labels, and event detection. Meanwhile, **specific** security mechanisms may be incorporated into an appropriate layer of the system to provide security services particularly to their needs, such as one security mechanism for each of the OSI architecture model.

  **http://codeidol.com/community/security/security-mechanisms/22778/

- Explain the following malware types: virus, worm, trojan horse, logic bomb.
  - **Virus**: A type of malware that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them. Viruses need a host to spread, such as via infected emails or softwares.
  - **Worm**: Worms are similar to viruses, except that they do not need hosts to spread, they spread on their own, by replicating themselves and using memory.
  - **Trojan horse**: A program designed to breach the security of a computer system while performing harmless functions.
  - **Logic bomb**: A set of instructions secretly incorporated into a program so that if a particular condition is satisfied, they will be carried out with harmful effects.

- Explain the following attack types: dictionary attack, replay attack, password sniffing, spoofing, denial of service.
  - **Dictionary attack**: An attempt to gain access to a computer system by using a very large set of words to generate potential passwords (i.e. testing each word in the hopes that one of them is the correct one).

- **Replay attack:** An attack that uses data from an earlier, recorded, valid session.
- **Password sniffing:** It has access to and monitors any valid session that contains a password.
- **Spoofing:** A malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver (e.g. the sender of an email listed as 'Facebook' or a service that the user uses); also known as *phishing*.
- **Denial of service:** An attack where the aim is to make the machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. For example, sending a spoofed packet (the victim is shown as the source) to many hosts, and the responses overwhelming the victim.

- Explain the following terms: injection attack, rootkit, social engineering.
  - **Injection attack:** It exploits the input vulnerability of data not being checked or sanitised properly (e.g. SQL statements inserted into an entry field for execution).
  - **Rootkit:** A malware that hides its presence behind an existing software via modifying the system data; enables an unauthorised user to gain control of a computer system without being detected.
  - **Social engineering:** It exploits human gullbility to extract confidential information (e.g. the attacker might pretend to be a co-worker with an urgent problem that requires access to additional network resources).

LECTURE 3

- What is encryption? What is the role of an encryption key?

  Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). **Encryption key** is the parameter that enables to translate the same plaintext with the same algorithm to different ciphertexts.

- What is the basic difference between symmetric key encryption and asymmertric key encryption?

  Symmetric key encryption uses identical key to both encrypt and decrypt the data (i.e. the encryption key can be calculated from the decryption key), while **asymmetric** key encryption uses two related keys (a public key that is shared and a private key that is never exposed) for data encryption and decryption.

- Compare symmetric and asymmetric key encryption based on the keys, security, complexity, and speed.
  - **Keys:** Symmetric uses one (privately) shared key, while asymmetric uses one public key and one private key (like a PO box, the address is the public key and the actual key for the box is the private key, so A can send a message to B if they know the address of B, but only B can open the message using the matching key).
  - **Security:** Symmetric is not as secure as asymmetric because of the chance of the key being exposed.
  - **Complexity:** Symmetric is much simpler than asymmetric.
  - **Speed:** Asymmetric is slower than symmetric.

- What is a stream chiper and what is a block cipher?

  Stream chiper is a symmetric key chiper where the transformation depends only on the actual symbol one bit at a time, and it does not consider the previous or next symbol(s). Meanwhile, in **block chiper**, a key and algorithm are applied to blocks of data rather than individual bits in a stream.

- Explain each of the following methods, describe their characteristics, and most important features: AES, RSA, Diffie-Hellman.
  - **Advanced Encryption Standard (AES)**: A version of the Rijndael block chiper, with a block size of 128 bits (4 x 4 array of bytes) and key sizes of 128, 192, 256 bits (10, 12, 14 rounds of calculations). Each round of calculation has four steps:
    - **AddRoundKey** where each byte is combined (XOR) with the subkey.
    - **SubBytes** where there is non-linear subsitution of each byte by using a lookup table.
    - **ShiftRows** which cyclically shifts the bytes in each row by a certain offset.
    - **MixColumns** which combines the bytes in each column by using a linear transformation (in the last round is is replaced by another AddRoundKey).

- **Rivest-Shamir-Adleman (RSA):** One of the first public-key cryptosystems, where the encryption key is public and differs from the decryption key which is kept secret; based on the difficulty of factoring the product of two large prime numbers. It has key sizes of 1024 to 4096 bits with one round of calculation. It involves four steps:
    - Key generation: Generate a public key and a private key.
    - Key distribution: To enable the sending of encrypted messages, the public key is shared by the receiver to the sender, but the private key is kept secret.
    - Encryption: The sender encrypts the plaintext using the receiver's public key, then sends the ciphertext to the receiver.
    - Decryption: The receiver decrypts the ciphertext from the sender using their private key.

- **Diffie-Hellman:** It is an alogrithm used to establish a shared secret between two parties, primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms (uses public-key protocol to support symmetric key encryption).
    - The sender and receiver share a public base and public modulus
    - The sender has their own private key, and the receiver has their own private key.
    - Sender and receiver computes their public key using the public base, public modulus, and their own private key. The result (the public key) is then exchanged.
    - The sender and receiver then share the same secret value.

- Explain cipher block chaining.

  Chiper block chaining is when the plaintext is combined (XOR) with the previous ciphertext block and then encrypted. During decryption time, the block is decrypted and saved as chipertext for feedback until the next block is decrypted. A random *initialisation vector* (IV) is used to encrypt the first block.

- What is a hash (or secure digest) function and what are its main features?

  A **hash** function is a fixed-length pattern characterising an arbitrary-length message. It is usually used for digital signatures to protect messages from alteration. There two types of hash function:
    - **Non-keyed**: The function depends on the message alone, also known as message integrity code (MIC).
    - **Keyed**: The function depends on the message and on a secret key, also known as message authentication code (MAC).

- What is a digital signature? What is it for and how is it produced?

  Digital signature is a private encryption key used to verifity the authenticity of an information, so that the message cannot be falsified. For example, it is produced by encrypting a hash of the document with the signer's private key. The digital signature is then appended to the document before it is sent.

LECTURE 4

- What is the difference between identification and authentication?

  Identification aims to establish the identity of a user, a communcating peer, or a process, while **authentication** aims to verify the identification, that the user (/peer/process) is who/what they claim to be.

- What are the three main authentication factors? Give a real-life example of multifactor authentication.
  - Proof by **knowledge**: Something you know, e.g. username and password.
  - Proof by **possession**: Something you hold, e.g. debit card.
  - Proof by **property**: Something that defines you, e.g. fingerprint.

  An example for a **multifactor authentication** would be banking ATMs, where you would need proof of possession (your debit card) and proof of knowledge (your ATM pin) to access your account.

- What is single sign-on?

  In **single sign-on**, the user is authenticated once, and subsequent authentications are re-using the result without user interaction. This is done by the systems sharing the authentication database or exchanging security assertions.

- Explain the challenge-response authentication model. How is it used with password?

  Challenge-response authentication model is an authentication method that relies on proof by knowledge. Essentially, the server presents a challenge to the user, and the user answers the challenge; if the answer is correct, the user is authenticated. It is used with password by storing the password in hidden form (e.g. encrypted or as its hash value), then when the user enters a password, the system computes the hidden form and compares the calculated value with the stored one.

- Explain the difference between http Basic and http Digest authentication.

  http Basic forwards the password that the user puts in plain form, while **http Digest** only forwards the hash value of the password, therefore adding a security layer to protect the password.

- Explain the following three password protection methods: exponential backoff, blacklisting, reverse Turing test.
  - **Exponential backoff:** It increases waiting time after every failed attempt of authentication.
  - **Blacklisting:** It locks the account after a certain number of consecutive incorrect guesses.
  - **Reverse Turing test:** It asks the user to perform tasks only humans can do (differentiates between humans and computers apart).

- What is a one-time password? Explain one method of generating it.

  It is temporary password that is usually delivered to users before they generate their own password; valid of a single session or transaction, therefore resistant to replaying attacks. To generate it, we can use one of the following methods:

  - **Time-synchronised**: A piece of hardware (token) generates the password; the token needs an accurate clock synchronised with the server's clock, and the algorithm must tolerate limited clock drift.
  - **Mathematical algorithms**: Each password is generated from the previous one by calculating the hash of the previous one; passwords are used one at a time, working backwards through the list.

- What is biometric authentication? What is the difference between physiological and behavioural methods?

  Biometric authentication is a form of identity verification that relies on proof by property, which can only be used to authenticate human users. It measures physical charactersitics and evaluates them against a stored pattern (verification or identification).

  - **Physiological** is commercially available, and comprises of features such as the fact, fingerprint, handprint, or eye/retina print.
  - **Behavioural** is used mainly as an additional authentication factor, which requires signatures, voice, or keystroke dynamics.

- What is iris recognition use for in computing, and how?

  The iris is located in the eye in front of the lens, it controls the pupil size. Its textural complexity and variation across people postualtes its uniqueness to individuals. **Iris recognition** is implemented based on pattern matching. Its steps include:

  - Acquisition: Scanning of the iris of the user.
  - Segmentation: Isolating the iris from the environment.
  - Normalisation: Transforming the iris into polar coordinates.
  - Feature extraction: Encoding.
  - Matching: Quantifying individuality with a theoretical model.

- What are the main problems in fingerprint authentication?

  The main problems in **fingerprint authentication** include low-quality images (e.g. caused by dirt, skin textures), distortions (e.g. caused by pushing the finger against a surface), and negative connotations (e.g. the police, crime).

- What are the major issues in face recognition?

  Major issues in **face recognition** include the risk of disguises, as well as illumination in the photograph, facial expressions, and natural aging.

- What is an X.509 certificate for? What does it contain and how is it secured?

  It is a form of **electronic certificate** which is an electronic document to prove an identity or right to access certain resources. It contains detailed information about the subject, and is issued by trustworthy authorities who are reputable themselves (a Certificate Authority). It is secured using public key encryption to identify the issuer and the subject, as well as to protect the content. Specifically for **X.509 certificate**, it contains the following information:

  - Version
  - Serial number
  - Signature algorithm ID
  - Issuer name
  - Validity period
  - Subject name
  - Subject public key info
  - Issuer unique ID
  - Subject unique ID
  - Extensions
  - Subject and issuer attributes
  - Key usage and policies
  - Certification path constrains

  *Version 1 (1988), Version 2 (1993), Version 3 (1996)

- What is a Certificate Revocation List?

  Certificate Revocation List is a list of invalid certificates.

- Explain the role of a Certificate Authority in Public Key Infrastructure.

  The role of **Certificate Authority** (CA) in public key infrastructure is to check the subject's details and sign certain type of certificates (depending on their level of authority). A Certificate Authority can delegeate the right of doing so to another CA, and the delegate can do the same thing.